REMARKS

Claims 11-14, 16, 17 and 19-24 have been presented for examination. Claims 5, 6, 11-14, 16 and 19 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,930,479 to Hall. Claims 1-4, 7, 8 and 20-24 have been rejected under 35 U.S.C. § 103(a) as being obvious over the patent to Hall in view of U.S. Patent No. 5,931,905 to Hashimoto *et al.* Claim 10 has been rejected as being obvious over the patent to Hall in view of U.S. Patent No. 6,092,101 to Birrell *et al.* further in view of a publication by Microsoft Corporation entitled "Excerpts from online documentation of Microsoft Exchange." Claim 17 has been rejected as being obvious over the patent to Hall in view of the patent to Birrell *et al.* further in view of U.S. Patent No. 5,619,648 to Canale.

The disclosed embodiments of the invention will now be discussed in comparison to the applied references. Of course, the discussion of the disclosed embodiments, and the discussion of the differences between the disclosed embodiments and the subject matter described in the applied references, do not define the scope or interpretation of any of the claims. Instead, such discussed differences merely help the Examiner appreciate important claim distinctions discussed thereafter.

The disclosed invention relates to a method and system for directing received e-mail messages to one of at least two user folders depending upon the identity of the e-mail sender. In the disclosed embodiment, a list is maintained containing information that identifies senders who are authorized to send an electronic mail message to the user. As explained below, the list of authorized senders allows the user to easily avoid reading e-mail messages from unauthorized senders even if the identity of the unauthorized senders is unknown. Thus, an unauthorized sender cannot circumvent the disclosed system and method by simply changing his or her e-mail address. When each e-mail message is received, the list is checked to determine whether the identification of the sender in the e-mail message is included in the list. If so, the sender of the e-mail message is considered to be authorized. If the sender of the e-mail message is determined to be authorized, the e-mail message is stored in a corresponding folder, such as an authorized message inbox. If no determination has been made that the sender of the e-mail message is authorized, the e-mail message is stored in a folder specifically designated for storage of e-mail messages from unauthorized senders. As a result, is not necessary for the user to scroll through a list of unauthorized messages to access authorized messages. However, the unauthorized e-mail messages are not automatically destroyed or deleted so that an unauthorized e-mail message can subsequently be read if desired.

None of the references cited by the Examiner disclose or suggest the system or method described above. The principal references cited by the Examiner is the patent to Hall and the patent to Hashimoto *et al.* The Hall patent discloses an e-mail communications system in which e-mail messages from unauthorized senders can be filtered out if identifying information contained in the sender's e-mail address is not in a list of authorized senders. The Examiner acknowledges that the Hall patent does not explicitly disclose storing the e-mail message in a first folder when a determination has been made that the e-mail message is from an authorized sender and storing e-mail message in a second folder when a determination has been made that the e-mail message is from an unauthorized sender.

The Examiner proposes to supply the teaching that is admittedly missing from the Hall patent by relying on the Hashimoto *et al.* patent, particularly at columns 12 and 13. According to the Examiner, Hashimoto *et al.* teach the system in which:

> [i]f the user ID has been registered in the list the e-mail is sent to the receiver's mailbox (first folder) and if the user ID of the sender is not registered in the authorized sender list, *the e-mail is abolished (deleted folder, second folder)* (col. 12, line 67-col. 13, line 4)."

(Emphasis added). However, this is not what is stated in column 12, line 67 through col. 13, line 4 of the Hashimoto *et al.* patent. Instead, this portion of the Hashimoto *et al.* patent states:

> [if] the user ID has been registered, a mail is sent similarly to the first embodiment. [*i.e.*, the e-mail is sent to the receiver's mailbox (first folder)]. If the user ID of the sender is not registered in the authorized sender list, present mail data is abolished and *abolition is notified to the sender.*

(Emphasis added). Thus, Hashimoto *et al.* do not teach or suggest sending an unauthorized e-mail to a deleted message folder or any other folder. Instead, Hashimoto *et al.* disclose simply destroying the e-mail. As a result, it would not be possible to read the unauthorized e-mail as an applicant's disclosed system. While notice of the e-mail destruction might be stored in a folder, it is stored in the folder of the sender since the only teaching of the Hashimoto *et al.* patent is that the sender is notified of the abolition or destruction of the e-mail. There is no suggestion in either the Hall or the Hashimoto *et al.* patent that the receiver is even in notified that the e-mail message was ever received or destroyed. Therefore, the Hashimoto *et al.* patent in combination with the Hall patent fails to suggest the basic concept of applicant's disclosed system and method, as described above.

The patent to Birrell *et al.* has been cited for disclosing a system for filtering unauthorized messages by labeling the messages as unread in the receiver's inbox. The Microsoft Corporation reference has been cited for the same purpose. Applicant acknowledges that labeling messages as unread in an inbox is old. Significantly, neither the Birrell *et al.* patent nor the Microsoft Corporation reference supplies the teachings that are missing from the Hall and Hashimoto *et al.* patents, namely storing unauthorized messages in a dedicated folder. The patent to Canale likewise fails to teach the basic concept of applicant's method and system as described above.

Turning, now, to the claims, claim 1 specifies a method for filtering unauthorized e-mail messages in which each e-mail sender has an identification that is included in the e-mail message. A method includes providing a list of the identification of authorized e-mail senders, and, for each of a plurality of e-mail messages, determining whether the sender of the e-mail message is authorized by determining whether the identification of the e-mail sender is provided in the identification list. When the sender of the e-mail message is determined to be authorized, the message is stored in a first folder designated for sent messages. However, when the sender of the e-mail message is determined to be not authorized, the e-mail message is stored in a "second folder designated for electronic mail messages received from unauthorized senders." As explained above, none of the cited references taken either alone or in combination disclose or suggest the method of claim 1, particularly with respect to storing unauthorized messages in a folder designated for e-mail messages from unauthorized senders.

Amended claim 5 is also directed to a method for filtering unauthorized messages. The method includes, for each of a plurality of messages, determining whether the sender of the message is designated as being authorized. When the sender of the message is determined to be authorized, an indication is provided that the message is from an unauthorized sender. Significantly, when the sender of the message is determined to be not authorized, the message is stored in a pre-designated location for messages sent by unauthorized senders. Again, none of the cited references disclose storing unauthorized messages in a designated location, such as a folder. Instead, the prior art suggests either storing messages from unauthorized senders in either the same folder that messages from authorized senders are stored, albeit with a indication that the messages are from an unauthorized sender, or simply deleting the unauthorized messages. In the first case, the user must scroll through both unauthorized and authorized messages, and, in the second case, the user may never know that an unauthorized message was received and may never be able to read it.

Finally, amended claim 20 specifies an e-mail system containing a receiving component receiving e-mail messages that include the identification of the e-mail message sender. The system also includes an authorized sender list having the identification of senders who are authorized to send e-mail messages. The system also includes an authorization component that is forwarded e-mail messages from the receiving component. The authorization component forwards the e-mail messages to a predetermined folder when the indication of the sender of the forwarded e-mail message is not in the authorized sender list. As explained above, none of the cited references either alone or in combination disclose the subject matter of claim 20.

The claims dependent on the above-discussed independent claims also patentably distinguish over the cited references because of their dependency unpatentable independent claims and because of the additional limitations added by those claims.

Insofar as all of the claims in the application patentably distinguish over the cited references, favorable consideration and a Notice of Allowance are earnestly solicited.

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned **"<u>Version with Markings to Show Changes Made</u>"**.

Respectfully submitted,

DORSEY & WHITNEY LLP

Edward W Bulchis

Edward W. Bulchis
Registration No. 26,847

EWB:dms

Enclosures:
Postcard
Fee Transmittal Sheet (+ copy)
General Authorization

1420 Fifth Avenue, Suite 3400
Seattle, WA 98101-4010
(206) 903-8800 (telephone)
(206) 903-8820 (fax)
h:\ip\documents\clients\micron technology\100\500122.02\500122.02 amendment 2nd oa.doc

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Claims:

Claims 7, 19 and 24 have been cancelled.

Claims 5, 8, 17, 20 and 23 have been amended as follows:

5. (Amended) A method in a computer system for filtering unauthorized messages, each message having a sender, the method comprising:

for each of a plurality of messages,

determining whether the sender of the message is designated as being authorized;

when the sender of the message is determined to be authorized, indicating that the message is from an authorized sender; and

when the sender of the message is determined to be not authorized, ~~[indicating that the message is from an unauthorized sender]~~storing the message in a pre-designated location for messages sent by unauthorized senders.

8. (Amended) The method of claim [7]5 wherein the message is an electronic mail message and the pre-designated location is a folder.

17. (Amended) The method of claim 5 [wherein the indicating that the message is from an unauthorized sender includes]further comprising forwarding the message from an unauthorized user to another user.

20. (Amended) An electronic mail system comprising:

a receiving component that receives electronic mail messages that include the identification of the sender of the electronic mail message;

an authorized sender list having the identification of senders who are authorized to send electronic mail messages; and an authorization component that is forwarded electronic mail messages from the receiving component and that [provides an indication]forwards the electronic mail messages to a predetermined folder when the identification of the sender of the forwarded electronic mail message is not in the authorized sender list.

23. (Amended) The system of claim 20 wherein the [provided indication is the storing of the forwarded electronic mail message in]predetermined folder comprises a junk mail folder.

H:\IP\Documents\Clients\Micron Technology\100\500122.02\500122.02 amendment 2nd OA.doc